

Crime Watch News

Long Beach Police Department . Crime Prevention Unit . 100 Long Beach Blud . Long Beach, CA 90802

Anthony W. Batts Chief of Police

Ted Hulsey

Deputy Chief of Police Patrol Bureau

Robert Luna

Deputy Chief of Police Investigations Bureau

Tim Jackman

Deputy Chief of Police Support Bureau

Braden Phillips

Manager Administration Bureau

Karen Owens

Administrator
Community Relations Division

Kevin Coy

Sergeant
Crime Prevention Unit
Community Relations Division

INSIDE THIS ISSUE

Upcoming Events and Volunteer Opportunities	.,1
Advisory Group Conference Debrief	. 2
37th Annual Police Awards Luncheon	. 2
Thieves Go "Phishing" For Your Identity	3
Neighborhood Watch Success Stories	4

COMMUNITY CRIME PREVENTION MEETING

SPECIAL WEAPONS AND TACTICS (S.W.A.T.)

Wednesday May 18, 2005 7:00 p.m.

Long Beach Water Department 1800 East Wardlow Road

Join us for a special evening with our S.W.A.T. Team Members.

Learn more about these well-equipped, specialized teams who are trained to respond to criminal acts and potential terrorist threats to our community.

The SWAT Team will be displaying their new tactical vehicles, so you might want to arrive a few minutes early!

Bring your family and friends!

UPCOMING EVENTS/VOLUNTEER OPPORTUNITIES



- Tuesday, May 17, 2005, 11:15 a.m.

 37th Annual Long Beach Police Awards Luncheon
 Long Beach Convention and Entertainment Center
 For further information, call: (562) 570-7215
- ◆ Saturday, May 21, 2005, 1:00 p.m. 5:00 p.m.
 Rape Prevention & Self Defense 101: Workshop for College Bound Students & Parents Long Beach City College, Pacific Coast Campus Gymnasium 1305 E. Pacific Coast Highway, Long Beach For further information, contact Sexual Assault Crisis Agency (SACA): (562) 494-5046
- ◆ Tuesday, May 10th, 5:00 p.m. Open Admission to the Aquarium, Meeting 7:00 p.m. Police Chief's Gay, Lesbian, Bisexual & Transgender Advisory Group Town Hall Meeting A Forum on Violent Crime and Hate Crimes within the Gay and Lesbian Community Long Beach Aquarium of the Pacific, 100 Aquarium Way For further information, contact the Community Relations Division: (562) 570-7215
- ◆ Sunday, June 5, 2005, 7:30 a.m. 4:00 p.m.
 10th Annual CPR Sunday & Health Expo
 Long Beach City College, Liberal Arts Campus, 4901 E. Carson Street, Long Beach For further information, contact The American Red Cross: (562) 490-4035

ADVISORY GROUP CONFERENCE DEBRIEF

SATURDAY, APRIL 30th

We'd like to offer a special thanks to all of the Chief's Advisory Group members that attended this past Saturday's Chief's Advisory Group Conference! You all did a great job of "Networking, Networking, Networking!" Also, a special thanks for the assistance from Rene Castro and the National Conference for Community and Justice (NCCJ).

We started out the day at 8:30 a.m. in the comfort of the Long Beach Water Department's Water Treatment Plant Community Room. (Don't worry, your water is fine....we had plenty of uniformed personnel and plenty of good people in attendance!) The following were the objectives for the day:

- To provide an opportunity for additional networking
- To continue to learn from one another the strategies to increase the role of communication between the Advisory Groups and the community
- To be provided an update on the Community Oriented Public Safety (COPS) Program
- To begin a dialogue on community participation in anti-terrorism efforts

After brief introductions of everyone present, Chief Batts arrived to provide an insightful and informative welcome with an update on the department. Then we went directly into our Advisory Group Updates in an effort to let everyone know what each group has been up to. We shanghaied a representative from each Advisory Group and brought them to the front to be interrogated by Police Service Assistants John Houck and Doris Thompson. Questions that were asked of the Advisory Groups:

- What are some ways that you are sharing information with your constituents?
- What have your groups been up to?
- Successes and Challenges
- What's planned for the future?

The groups have been busy! Just a few, but not all of the responses were:

Women's:

Cell Phone Drive Denim Day Rape Awareness Forum

Gay, Lesbian, Bisexual, Transgender:

Gay and Lesbian Forum at the Aquarium of the Pacific

Academic:

Advisory Group Website

African-American:

Civil Service Recruitment

Seniors:

Senior Notification Flyer

Latino:

Helping to plan the 1st Latino Community Academy

All the groups are doing a great job and are to be commended for their volunteer efforts to help educate their respective communities.

The groups were then shown a counter-terrorism video, the "7-Signs of Terrorism." It's an eye-opening video developed in Michigan to educate the public on terrorism awareness. At the end of the video, the participants broke out into their respective groups for a brainstorming session. groups were then asked to brainstorm the methods used by each Advisory Group to disseminate police department information to their respective communities. It was a good learning experience and one we will revisit again to help the groups disseminate information to their communities.

Many thanks to all members who participated this past Saturday! We appreciate all you do!

Advisory Group Members

Save the date for our next conference! Saturday, October 1st 8:30 a.m. to 12:30 p.m.





37TH ANNUAL POLICE AWARDS LUNCHEON

Tickets Nearly Sold Out!

It's not too late to purchase your tickets to attend the 37th Annual Police Awards Luncheon to be held on Tuesday, May 17, 2005, 12:00 noon, at the Long Beach Convention and Entertainment Center.



Special Guest Narrator Jennifer Bjorklund NBC 4 News

This luncheon publicly honors those brave citizens and police employees who have distinguished themselves by aiding their fellow men and women, often at great risk to their own personal safety.



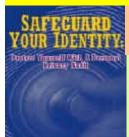
Special Guest Narrator Gordon Tokumatsu NBC 4 News

Don't Delay! Tickets will be available for purchase up until

Thursday, May 12, 5:00 p.m.

in the Community Relations Division, 333 W. Broadway, Suite 100.

\$30 each or \$300 for a table of 10



THIEVES GO "PHISHING" FOR YOUR IDENTITY

CRIME PREVENTION UNIT CORPORAL, HARRY ERICKSON

Have you been phished, spoofed, cloaked or cloned lately? These are all the latest hi-tech

terms associated with the current methods of Identity Theft.

A large number of our population utilizes e-mail on a daily basis. It is a fast, effective and convenient way of communicating with friends, family and business associates. If you have an e-mail account, chances are you have been the target of "phishing" in the recent past. The term phishing is a variation of the word fishing as in "fishing for information", used by computer hackers. A phishing scam utilizes an e-mail message to trick victims into revealing their personal financial information, ultimately leading to identity theft.

The Lure - The perpetrator first sets up a "clone" of a reputable company's website, utilizing actual graphics, font style, color scheme and logos to make a copy of that company's website. They then pose as the reputable company and send out thousands or even hundreds of thousands of random e-mail messages to potential victims. The message appears to be from the legitimate company. One such actual case involved the use of the Visa Credit Card Company name. The email appeared to be from "notification@visa.com." This is a very simple technique called "spoofing," which can be done from most computers, by someone with basic computer knowledge. Most of the people who receive the e-mail don't even have an account with the company who it appears to be from. However, based on the large volume of e-mails sent out, and the large customer base of the spoofed company, there is likely a good number of people who do have an account with that company. Even if, out of the thousands of e-mails sent, only a few people fall for the scheme, the scam pays handsomely for the thief.

The Hook - The unsuspecting victim thinks that they have received a legitimate notification from their bank or other company whom they do business with. The victim clicks on a link within the e-mail message. which appears to direct them to the real company's website. Remember, the thief has already set up a clone of the real company's website somewhere out in cyberspace. Even the address in the browser bar appears to be that of the legitimate company. This is called "cloaking." The link is disguised something like "www.visa.com," but really directs the victim to the thief's cloned copy website. Once the victim is at the cloned website, there is a form for him/her to fill out, asking to verify or update their account information. Some phishing scams simply integrate graphics and a form into the e-mail message, eliminating the need to set up a cloned website.

The Catch - After the victim fills out the form and clicks "send," the information is sent to the thief. The thief then uses the information to open bank and credit card accounts and makes purchases under the victim's name. The thief may also sell the victim's information to other thieves. The thieves and computers used to com-

mit these crimes can be stationed anywhere in the world, making apprehension and prosecution very difficult.



Protecting Yourself

 If you receive an e-mail asking you for personal or financial information, do not click on any links or fill out any forms within that email. Legitimate companies will not request this information via e-mail.

Protecting Yourself (continued)

- If you get an e-mail which appears to be phishing for information, forward a copy to the Federal Trade Commission at spam@uce.gov.
- Be cautious of opening any attachments within emails, regardless of who they appear to be from. These attachments can contain spyware or viruses which can monitor your computer activity without your knowledge.
- Use firewall and anti-virus software to protect your computer. They will not protect you from phishing scams, however, they are good at protecting you against virus and spyware intrusion.
- If you wish to make a purchase online, make sure you are buying from a reputable company through a secure website. Secure web pages begin with "https" and there will be a security lock icon near the lower right area of your browser. Unfortunately, this can be forged as well, however, if you initiate the transaction with a known reputable company on their secure website, your information should be safe.
- Finally, if you think you have been the victim of a phishing scam, notify your bank and credit card companies right away and check your credit report for suspicious activity.

For more information on Identity Theft or other crime prevention topics, contact the Long Beach Police Department's Crime Prevention Unit.



NEIGHBORHOOD WATCH SUCCESS STORIES

This month's success story arrived with perfect timing to go along with our article on Internet "Phishing." It's a crime that can affect anyone with an e-mail account. Read on to see how Neighborhood Watch takes a bite out of Internet schemes!

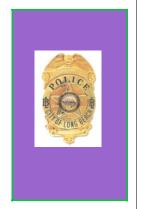
Forward your Neighborhood Watch Success Stories to PSA Lisa Massacani at Lisa_Massacani@longbeach.gov.

Block Captain Sharman Wallace keeps her Neighborhood Watch Group current on the latest in crime prevention by scheduling regular meetings with her neighbors. Recently, this training prevented a neighbor, Mr. Spencer Leister, from becoming yet another victim of Internet fraud. When he received a suspicious e-mail on April 6th, he put his training to use and thwarted a possible identity theft attempt.

The subject line of the e-mail read, "Unauthorized Access To Your Washington Mutual Internet Banking Account." The message stated the bank had recently reviewed Mr. Leister's account and suspected the account may have been accessed by a third party. Mr. Leister was directed to restore his account access by clicking on a provided Internet link. He was instructed to enter his social security number in both the personal identification and password boxes. He was then instructed to fill in additional "required" information, including his full name and account number.

Mr. Leister immediately became suspicious. He new he should not provide his personal information because he had just attended one of Sharman's Neighborhood Watch meetings with a presentation on Identity Theft and Fraud. Instead of following the instructions to click on the provided links, he called the bank. The bank advised him that the message was fraudulent and provided a phone number to report the incident. After following through with the report, Mr. Leister notified his Block Captain, who passed the alert to others in their Neighborhood Watch Group.

Violent crimes usually make the biggest headlines, but Internet crimes occur much more frequently and within the safety of our own homes. Education is the most effective tool to prevent us from falling victim to these crimes. To keep your Neighborhood Watch group current on the latest schemes, schedule a Neighborhood Watch meeting by calling PSA Lisa Massacani at (562) 570-7229.



Long Beach Police Department Community Relations Division 100 Long Beach Boulevard Long Beach, CA 90802



Internet Reader